REMARKS

Applicants appreciate the Examiner's attention to this application.

This response cancels claims 1-2, 15, 18, and 21; amends claims 3-7, 10-11, 13, 16, 19, and 23; and adds claim 24. Claims 10, 19, and 24 are the pending independent claims. Reconsideration of the present application in view of the enclosed amendments and remarks is respectfully requested.

ARGUMENT

The Office Action includes claim rejections based on 35 U.S.C. §§ 102(b) and 103(a). To the extent that those rejections might be applied to the claims, as amended by this response, Applicants respectfully traverse.

35 U.S.C. § 102(b)

The Office Action rejects claims 1, 6, 16, and 19-20 as being anticipated by U.S. patent no 5,825,880 to Frank W. Sudia et al. (hereinafter "Sudia"). For a valid rejection under 35 U.S.C. § 102, "[t]he identical invention must be shown in as complete detail as is contained in the ... claim." (MPEP § 2131.01, quoting from Richardson v. Suzuki Motor Co., 9 USPQ2d 1913, 1920 (Fed. Cir. 1989)).

Sudia pertains to a multi-step signing process, in which multiple signing devices each provide a "partial signature," and the partial signatures are combined to form a "final signature" (Abstract).

In the present application, the pending independent claims (i.e., claims 10, 19, and 24) all involve isolated execution mode. As recognized in the Office Action, Sudia "does not disclose 'a processor running in isolated execution mode.'" Sudia therefore does not anticipate any of the pending independent claims.

35 U.S.C. § 103(a)

The Office Action rejects claims 2, 10-15, and 17-18 as being unpatentable over Sudia, in view of U.S. patent no. 4,403,283 to Jon N. Myntti et al. (hereinafter "Myntti"). Myntti pertains to a memory system that maps different user programs into mutually exclusive portions of physical memory (referred to as "real memory"). In particular, Myntti pertains to systems that support more real memory than can be addressed directly by a processor. For example, Myntti describes a system that uses a 16-bit processor, which can directly access only 65,536 (64K) words of memory. However, the system also includes real memory that is much larger than 64K. In such a system, Myntti suggests establishing a translation table for mapping the "logical addresses" used by different programs to different physical addresses. For example, two different user programs that use 16-bit memory addressing can both refer to the same 16-bit logical address, but the translation table would map the logical memory references from each user program to different real (i.e., physical) addresses.

Neither Sudia nor Myntti provides any motivation to combine Sudia and Myntti. Furthermore, even if Sudia and Myntti were to be combined, the combination would not render the pending claims unpatentable. Such a combination, assuming it could be made to work, would merely create an environment with multiple different signing devices, as per Sudia, where one or more of the systems in the environment maps the logical memory addresses used by different user programs to different areas of physical memory, as per Myntti.

By contrast, claim 24 of the present application pertains to a platform that includes a processor that can operate in a "normal execution mode" and in an "isolated execution mode." A platform according to claim 24 also features a system memory to include "an isolated area that is accessible only when the processor is operating in isolated execution mode." As explained in the detailed description of the present application, isolated execution mode is a mode of operation in which the platform allows access to a region of system memory

that is protected by the platform hardware. Such regions of memory may be referred to as "isolated memory areas" or simply "isolated memory." The platform hardware prevents access to isolated memory when the system is not in isolated execution mode (e.g., when the system is in "normal execution mode"). Furthermore, isolated execution mode is not to be confused with conventional privilege rings. For example, as explained in greater detail in the detailed description, a platform that supports a "normal execution mode" and an "isolated execution mode" may also support privilege rings within the normal execution mode, as well as privilege rings within the isolated execution mode. (FIGs. 1A-1C and page 5, line 5, through page 10, line 21.)

Sudia does not disclose or suggest a processor to operate in isolated execution mode. The Office Action asserts that column 6, lines 19-28 of Myntti teaches "a processor running in isolated mode." Applicants respectfully traverse that assertion. That portion of Myntti does not disclose or suggest "a processor to operate selectively in distinct modes including a normal execution mode and an isolated execution mode," as recited in claim 24. Instead, the cited portion of Myntti merely indicates that, by mapping the logical addresses of different user programs to different physical addresses, "each user program is 'isolated' from execution of each other user program." The mapping of Myntti has nothing to do with a processor operating in isolated execution mode. The processor of Myntti presumably is only capable of supporting normal execution mode. For instance, column 4, line 55, through column 5, line 17, describe part of the memory mapping process, with regard to "a typical 16 bit logical address produced by processor 9." Those lines do not disclose or suggest "a processor to operate selectively in distinct modes including a normal execution mode and an isolated execution mode," as recited in claim 24.

Consequently, even if Sudia and Myntti were to be combined, the combination would not establish a *prima facie* case of obviousness for claim 24. In addition, claims 10 and 19 involve features that are similar to those of claim 24 described above, and the remaining claims depend ultimately from claim 10,

claim 19, or claim 24. A combination of Sudia and Myntti therefore would not establish a *prima facie* case of obviousness for any of the pending claims.

The Office Action rejects claims 3-5, 7-9, and 22-23 as being unpatentable over Sudia, in view of U.S. patent no. 6,609,199 to John DeTreville (hereinafter "DeTreville"). The Office Action rejects claims 8 and 9 as being unpatentable over Sudia, in view of U.S. patent no. 6,108,644 to David M. Goldschlag (hereinafter "Goldschlag"). To the extent that any of those rejections might be applied to the pending claims in the present application, Applicants respectfully traverse.

In the present application, the pending independent claims (i.e., claims 10, 19, and 24) all involve isolated execution mode. Neither DeTreville nor Goldschlag disclose or suggest the concept of isolated execution mode. As indicated above, neither does Sudia. Consequently, even if Sudia were to be combined with DeTreville or Goldschlag, the combination would not establish a *prima facie* case of obviousness for any of the independent claims. Since the dependent claims implicitly include the features of their respective parent claims, a combination of Sudia and DeTreville, or Sudia and Goldschlag, would not establish a *prima facie* case of obviousness for any of the pending dependent claims.

For reasons including those set forth above, the Office Action fails to make out a *prima facie* case of obviousness for any of the pending claims. For these and other reasons, all pending claims are allowable.

CONCLUSION

In view of the foregoing, claims 3-14, 16-17, 19-20, and 22-24 are all in condition for allowance.

If the Examiner has any questions, the Examiner is invited to contact the undersigned at (512) 732-3927. Early issuance of Notice of Allowance is respectfully requested.

Respectfully submitted,

Dated: 8/3/04

Michael R. Barré
Patent Attorney
Intel Americas, Inc.
Registration No. 44,023
(512) 732-3927

c/o Blakely, Sokoloff, Taylor &
Zafman, LLP
12400 Wilshire Blvd.
Seventh Floor
Los Angeles, CA 90025-1026